PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-251326
(43)Date of publication of application : 06.09.2002

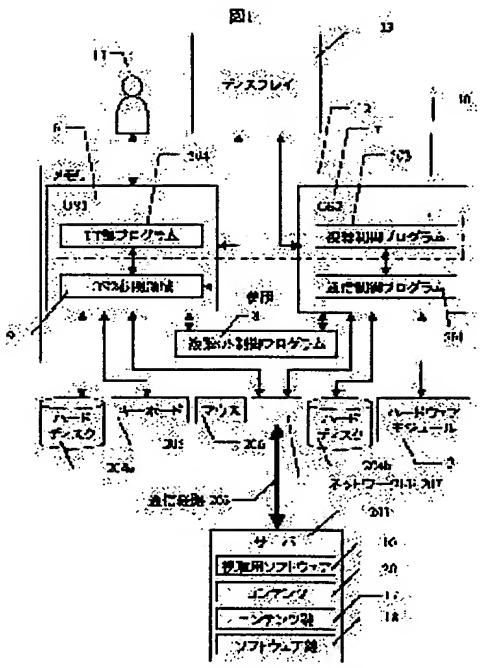
(51)Int.CI. G06F 12/14
G06F 1/00
G06K 19/00

(21)Application number : 2001-045949
(22)Date of filing : 22.02.2001

(71)Applicant : HITACHI LTD
(72)Inventor : ITO SHINJI
YOSHIURA YUTAKA
OKAMOTO HIROO

(54) TAMPER-PROOF COMPUTER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system and a method on a PC for realizing a system capable of preventing static and dynamic analyses and alterations by a user of software that operates on a PC.
SOLUTION: Two OSs being an OS1 that can be operated by a user and an OS2 that operates in the background are made to simultaneously operate on the PC. Audio-visual software 10 is prevented from being analyzed and tampered by the user 11 by operating the audio-visual software 10 on the OS2. Activation of the system and management of a key are also performed by using a hardware module 3. Furthermore, the OS1 indirectly accesses the OS2 by eliminating direct access from the OS1 to the OS2 and allowing the OS2 side to refer to the OS2 reference area 9 of the OS1 side.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－251326
（P2002－251326A）
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
			３２０Ｂ	５Ｂ０３５
1/00		9/06	６６０Ｇ	５Ｂ０７６
Ｇ０６Ｋ　19/00		Ｇ０６Ｋ　19/00	Ｑ	

審査請求　未請求　請求項の数５　ＯＬ　（全 15 頁）

(21)出願番号　特願2001－45949(P2001－45949)

(22)出願日　平成13年２月22日(2001.2.22)

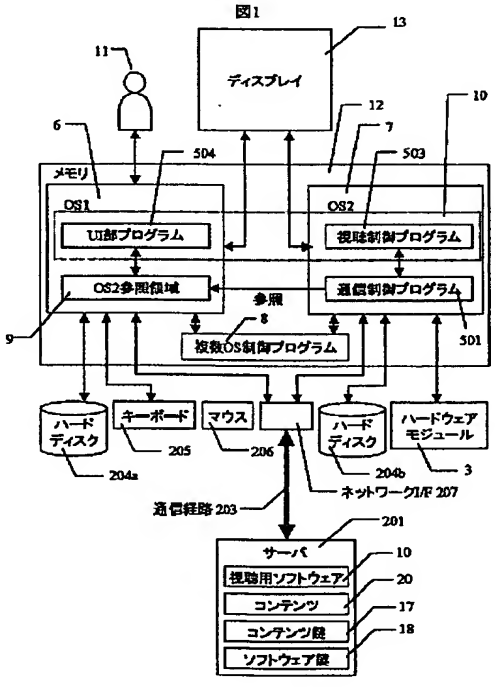
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　伊藤　信治
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　耐タンパ計算機システム

(57)【要約】
【課題】ＰＣ上で動作するソフトウェアのユーザによる静的及び動的な解析、改ざんを防止可能なシステムをＰＣ上で実現するシステム及び方法を提供する。
【解決手段】ＰＣ上にユーザが操作可能なＯＳ１とバックグランドで動作するＯＳ２の２つのＯＳを同時に動作させる。視聴用ソフトウェア１０をＯＳ２上で動作させることにより、ユーザ１１による視聴用ソフトウェア１０の解析、改ざんを防止する。また、ハードウェアモジュール３を用いて、システムの起動および鍵管理を行う。さらに、ＯＳ１からＯＳ２への直接のアクセスをなくし、ＯＳ１側のＯＳ２参照領域９をＯＳ２側が参照することにより、間接的にＯＳ１からＯＳ２へアクセスを行う。

図1



1

【特許請求の範囲】

【請求項１】ＣＰＵと主記憶装置とを有し、アプリケーションソフトウェアを動作させる耐タンパ計算機システムであって、

第１と第２のＯＳを備え、

上記アプリケーションソフトウェアは、上記第１のＯＳ上で動作する第１の部分プログラムと、上記第２のＯＳ上で動作する第２の部分プログラムとからなり、

上記第１の部分プログラムは、当該計算機のユーザから操作を受け付けて上記第２の部分プログラムへコマンドを発行するユーザインタフェース部を備え、

上記第２の部分プログラムは、上記第１の部分プログラムが発行したコマンドの内、予め許可されたコマンドを実行し、

上記ユーザによる上記第２の部分プログラムへのアクセスまたは解析を防止する耐タンパ計算機システム。

【請求項２】請求項１に記載の耐タンパ計算機システムであって、

上記第２の部分プログラムは、コマンドを実行するコマンド処理プログラムと、

上記コマンド処理プログラムに、第１の部分プログラムが発行したコマンドの内、特定の許可されたコマンドを上記コマンド処理プログラムに送信する通信制御プログラムと、を備える耐タンパ計算機システム。

【請求項３】請求項２に記載の耐タンパ計算機システムであって、

さらに、上記第１と第２のＯＳを制御する複数ＯＳ制御プログラムを備え、

上記複数ＯＳ制御プログラムは、上記通信制御プログラムが上記第１のＯＳが管理するメモリ領域の特定領域を参照可能になるように設定し、

上記第１の部分プログラムのユーザインタフェース部は、上記特定領域にコマンドを書き込むことによりコマンドを発行し、

上記通信制御プログラムは、上記特定領域を参照して、上記第１の部分プログラムが発行したコマンドを読みとり、上記第２のＯＳが管理するメモリ領域内に備える許可されたコマンドリストを参照して、上記許可されたコマンドを上記コマンド処理プログラムに送信する耐タンパ計算機システム。

【請求項４】請求項３に記載の耐タンパ計算機システムであって、

耐タンパ性を有し、システム起動プログラムを格納するハードウェアモジュールを接続し、

当該耐タンパ計算機システムは、起動時に上記ハードウェアモジュールから上記起動プログラムを読み出す初期プログラムを備え、

上記起動プログラムは、上記複数ＯＳ制御プログラムを読み出して実行させる機能と、

上記複数ＯＳ制御プログラムは、上記第１のＯＳと上記第２のＯＳとを読み出して実行させる機能と、を備える耐タンパ計算機システム。

2

【請求項５】請求項４に記載の耐タンパ計算機システムであって、

上記第２の部分プログラムは、本体起動プログラムと暗号化ソフトウェアとディジタル署名とを備え、

上記ハードウェアモジュールは、上記暗号化ソフトウェアの復号化鍵と上記本体起動プログラムを認証する機能とを備え、

上記本体起動プログラムは、上記ハードウェアモジュールとの間で認証を行う機能と、上記ハードウェアモジュールから上記暗号化ソフトウェアの復号化鍵を取り出す機能と、取り出した上記復号化鍵を用いて上記暗号化ソフトウェアを復号化する機能と、を備え、

上記第１の部分プログラムから読み出したコマンドに従い、上記本体起動プログラムの実行と、上記暗号化ソフトウェアの復号化と実行とを行う耐タンパ計算機システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は計算機上で動作するソフトウェアの解析、改ざんを防止し、高い安全性を確保するための技術に関する。

【０００２】

【従来の技術】動画、静止画、音楽などのディジタルコンテンツを視聴するための再生装置には、著作権保護機能を持った専用ハードウェアを用いる場合と、著作権保護機能を持った視聴用ソフトウェアを用いる場合とがある。視聴用ソフトウェアを用いる場合には、通常パーソナルコンピュータ（以下、ＰＣという）のような汎用的計算機が再生装置として用いられるため、以下、ＰＣを例にして説明する。

【０００３】著作権保護機能を持った専用ハードウェアを用いた場合、コンテンツは暗号化して配布し、正規のプレーヤの、内部の解析、改ざんが困難な耐タンパモジュール内で暗号化コンテンツの復号を行い、利用条件などの付加情報の読み取りを行い、利用条件を満足する場合にのみ再生を行っている。

【０００４】ＰＣ上で著作権を保護しつつコンテンツの視聴を行う場合、視聴用ソフトウェアに著作権保護機能を付加することによりコンテンツの再生を行う。具体的には、コンテンツのストリーミング配信の場合は、コンテンツをユーザのＰＣ上に保存しないようにすることによって視聴する。または、暗号化されたコンテンツをユーザのＰＣに保存しておき、視聴するときは専用ハードウェアを用いる場合と同様に、暗号化コンテンツの復号、利用条件の読み取り、再生を行う。

【０００５】

【発明が解決しようとする課題】視聴用ソフトウェアの著作権保護機能などの改ざん及び解析を防止するために

は、これを暗号化してファイルに保存する方法と隠しファイルのような見えないファイルに保存する方法がある。上記の二つの方法の実行時には、メモリ内で暗号が解かれ、実行時には、隠しファイルの内容がメモリにロードされる。そのため、実行時にメモリが解析されるという懸念がある。同様に、コンテンツの不正コピーを防止するためには、視聴用ソフトウェアの場合と同様に、これを暗号化してファイルに保存する方法と隠しファイルのような見えないファイルに保存する方法がある。これらの方法についても、視聴用ソフトウェアの場合と同様の懸念がある。

【０００６】現状のＰＣは、専門の知識を持っている人であればオペレーティングシステム（ＯＳ）を操作したり、あるいは他のソフトウェアを導入することにより、ハードディスクなどに保存されている視聴用ソフトウェアを解析、改ざんを行うことが可能になる。そのため、保存できないように意図されているコンテンツを保存できるようにしたり、利用条件に反する利用を行ったり、あるいは私的利用のみ許されているコンテンツを他人が利用できるようにすることが可能であり、著作権を保護できなくなることが有り得る。

【０００７】専用ハードウェアを用いた場合には十分に著作権を保護することは可能であるが、端末がモデルチェンジした場合や付加された新しい機能を使おうとした場合にはユーザは新しい端末を購入する必要があり、負担を強いられる。今後、ますます多機能化が進むと予想され、これらの問題を克服して専用ハードウェアを常に最新の機能を利用可能な状態にするのは困難である。

【０００８】

【課題を解決するための手段】本発明は、ＰＣのような汎用的な装置上で動作する視聴用ソフトウェアを用いてコンテンツを視聴するコンテンツ視聴システム（以下、単にシステムという）において、コンテンツの著作権をより厳重に保護可能な技術を提供する。本発明は、ＰＣのような汎用的な装置上で動作する視聴用ソフトウェアの解析、改ざんを困難にする技術、システムを提供する。

【０００９】本発明の一態様では、以下の構成を提供する。ユーザが操作を行うユーザインタフェース処理に係わる環境１と不正操作から保護したい環境２という独立した２つの環境とそれらを接続する通信機能をＰＣなどの一台の装置上に設ける。それぞれの環境上で動作する処理ユニット（プログラム）が連携してアプリケーションソフトウェア（たとえば視聴用ソフトウェア）を構成する。不正処理を排除するために、環境１から環境２または環境２から環境１への通信を制限する通信制御機能を設定する。具体的には、以下のように行う。

【００１０】環境１から環境２への通信は、環境１側の視聴用ソフトウェアが通信のために設けた特定領域に、送信する命令または情報を書き込む。環境２側はこの特定領域を参照することにより命令または情報を受け取る。環境２側はあらかじめ環境２側で処理が許された命令または情報のリストを持ち、そのリストを参照して許された命令または情報に対する処理を行う。環境２から環境１への通信は環境２側の視聴用ソフトウェアが特定領域に命令または情報を書き込むことにより行う。環境１側ではこの特定領域を参照することにより命令または情報を受け取り処理する。以上のように環境２側が主導権を持つことにより、悪意を持ったユーザが環境１から不正操作を試みても排除することができる。

【００１１】さらに具体的には、環境１と２をそれぞれ独立したＯＳが管理することにより各環境の独立性を確保する。一台の装置で二つのＯＳを動作させるための管理とＯＳ間通信の管理とを行う複数ＯＳ制御プログラムを設ける。複数ＯＳ制御プログラムはＯＳ毎に独立したメモリ領域を割り当て、一方のＯＳから他方のＯＳのメモリ領域へのアクセスを防止する。本発明におけるＯＳとは、プロセス制御機能、プロセススケジューリング機能、割込み制御機能、メモリ管理機能を持つ。したがって、一般的にＯＳと呼ばれるものに限らず上記特徴を持つものであれば、本発明を適用することは可能である。

【００１２】視聴用ソフトウェアなどのアプリケーションソフトウェアについては、ユーザからの操作指示等の入力を受け取り、または、ユーザへのメッセージ出力を行う部分（ユーザインタフェース部）を環境１上に、実際にユーザからの操作指示を実行する部分（コマンド処理部、例えば視聴制御部）を環境２上にそれぞれ構成する。ユーザインタフェース部は環境１側でユーザからの操作を受け取り、上述した環境１と環境２間の通信機能に基づき、環境２側の視聴制御部にユーザからの操作を伝達し、コマンド処理部がユーザの操作に基づく処理を実行する。

【００１３】アプリケーションソフトウェアはＣＤ－ＲＯＭなどの可搬型記憶媒体を用いて、または他のサーバから通信媒体を用いてネットワーク経由で入手する。導入前のアプリケーションソフトウェアは、環境１上で動作する部分と環境２上で動作する部分と、ディジタル署名を持ち、環境１上で動作する部分のプログラムが、上述の環境１と環境２間の通信方法により、環境２側へインストール命令を送信する。環境２側では、ディジタル署名を用いて正規のアプリケーションソフトウェアであることを確認したら、インストールを行う。インストールとは、ソフトウェアをコンピュータ上で使用できるように組み込む作業を指す。

【００１４】システム起動、システムインストール、アプリケーションソフトウェアの使用許可、コンテンツの使用許可などのために、ＰＣと連携して動作する、物理的及び論理的に内部解析や改ざんを防ぐ耐タンパ性を備えた、ハードウェアモジュールを用いる。ハードウェアモジュールとは、たとえば、ＰＣの拡張ボードや、ＩＣ

カード（スマートカード）が該当する。

【００１５】視聴用ソフトウェアは一部または全部が暗号化されていてもよい。その場合は、視聴用ソフトウェアの入手とは別の機会に復号鍵を入手すればよい。たとえばＰＣと、復号鍵を供給するサーバとを通信路で接続し、認証後に、暗号化された通信路を用いてハードウェアモジュールがＰＣ経由で受け取ればよい。ハードウェアモジュールは視聴用ソフトウェアの暗号化された部分を復号する命令を受け取ることにより、環境２上で復号を行う。

【００１６】視聴用ソフトウェアは通常、ハードディスクなどの記憶装置上に保存するので、静的な解析を防止するために、一部を暗号化しておいてもよい。さらにディジタル署名を付加することにより、改ざんも防止可能である。視聴用ソフトウェアを暗号化した場合の復号鍵はハードウェアモジュール内に保存しておけばよい。

【００１７】視聴用ソフトウェアで処理するコンテンツは、必要に応じて暗号化して配布する。暗号化されたコンテンツの復号鍵は暗号化された視聴用ソフトウェアの復号鍵の入手方法と同様の方法により入手し、ハードウェアモジュール内に保存する。コンテンツを保存する場所は、環境１または環境２のどちらの領域であっても良いし、ハードウェアモジュール内に保存しても良い。

【００１８】ハードウェアモジュール内に保存する視聴用ソフトウェアまたはコンテンツの暗号化、復号化に用いる鍵にアクセスする際には、ハードウェアモジュールと環境２上で動作する視聴用ソフトウェアとが、ディジタル署名を用いた認証を行い、ハードウェアモジュールが正当であると認めた視聴用ソフトウェアがハードウェアモジュールへのアクセスを行う。これにより、ハードウェアモジュール内の情報を不正に取り出すことを防止可能である。

【００１９】システムを正常に起動させるために、起動プログラム（ブートプログラム）も上述の耐タンパ性を備えたハードウェアモジュール内にあらかじめ保存しておく。

【００２０】システム起動時には、まず、認証プログラムをＰＣのメモリ上にロードし、認証プログラムがメモリ上で他の不要なプロセス（たとえば、不正な解析プログラムなど）が動作していないことを確認した上で、ブートプログラムをＰＣのメモリ上にロードし実行する。ブートプログラムは複数ＯＳ制御プログラム、ＯＳ１とＯＳ２などのシステムファイルをハードディスクからメモリ上にロードし、必要に応じて、ハードウェアモジュールから暗号化されたシステムファイルの復号鍵を取り出し、ＰＣのメモリ上で復号する。復号後は、各ＯＳは初期設定などを行うことにより、システムの起動が終了する。上述の方法によれば、視聴用ソフトウェアを実行する際のメモリへのアクセスや解析が禁止あるいは制限されるので、視聴用ソフトウェアの改ざん及び解析を防止することや、コンテンツの著作権保護が可能となる。

【００２１】ハードウェアモジュールとしてＩＣカード（スマートカード）などのリムーバブル形式のものを用いた場合には、ハードウェアモジュールを持ち運ぶことによって、本発明のシステムが導入されている他の端末であっても視聴権のあるコンテンツを視聴することが可能である。

【００２２】上記説明では、コンテンツ視聴用ソフトウェアを例示したが、本発明は、これに限定されることなく、ＯＳ上で動作する、不正使用、改ざん、または不正解析の対象となりうる、あらゆるアプリケーションソフトウェアに適用できるものである。

【００２３】

【発明の実施形態】（システム概要）図１は本実施例のシステムの構成例である。本実施例のシステムは、１台のＰＣ上で複数ＯＳ制御プログラム８がＯＳ１とＯＳ２の２つのＯＳを制御する。１２はＰＣ上のメモリ領域であり、６はＯＳ１が管理するメモリ領域、７はＯＳ２が管理するメモリ領域、複数ＯＳ制御プログラム８のメモリ領域を持つ。ＯＳ１はハードディスク２０４ａ、キーボード２０５、マウス２０６を管理し、ＯＳ２はハードディスク２０４ｂ、ハードウェアモジュール３を管理する。ディスプレイ１３は複数ＯＳ制御プログラム８が表示の排他制御を行うことにより、ＯＳ１、ＯＳ２の両方から表示可能となっている。さらに、ディスプレイ１３と同様の排他制御によりＯＳ１、ＯＳ２の両方から出力できるスピーカを備えても良い。１０は視聴用ソフトウェアであり、ユーザインタフェース（Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ、以下ＵＩと称す）部プログラム５０４と視聴制御プログラム５０３及び、その他にも設定ファイルなどを持つ。

【００２４】複数ＯＳ制御プログラム８は、１台のＰＣ上で複数のＯＳが動作するための各種の制御をする部分で、各ハードウェアの初期化および分割占有処理、ＯＳ単位でのＣＰＵのスケジューリング、割り込み処理などを行う。

【００２５】各ＯＳはそれぞれ仮想アドレスを実アドレスに変換するためのテーブル（ページテーブルともいう）を持っている。特開平１１－１４９３８５号公報には、複数ＯＳ制御プログラム８がこれらのテーブルの切り替えを行うことにより、特権命令（ＯＳ以外では実行できないような保護機能や、メモリ管理機能の設定を行うためのもの）のエミュレーションを行わずに複数のＯＳを１台のＰＣ上で動作させる方法を開示している。その他、１台のＰＣ上に複数のＯＳを同時に動作させるための技術としては、ＰＣのハードウェアのエミュレーションを行う仮想計算機と呼ばれる技術がある。これらを本発明の前提条件として、以下説明する。

【００２６】本実施例において、２つのＯＳのうち、一方のＯＳ１はユーザが直接操作する機能を提供するが、

もう一方のＯＳ２はユーザ１１から直接操作する機能を提供しない。さらに、ＯＳ間の通信を制御することにより、ＯＳ１からＯＳ２への直接アクセス機能も提供しない。これらにより、ユーザがＯＳ２側で動作中のソフトウェアの詳細を知ることができないようにして、ＯＳ２側で動作中のソフトウェアをデバックするなどといった動的解析を防ぐ。

【００２７】このようなシステム構成のもと、視聴用ソフトウェア１０といった解析されたくないソフトウェアの、実際に視聴の制御を行う視聴制御プログラム５０３をＯＳ２上で動作させ、ユーザ１１からの操作情報を受け取るＵＩ部プログラム５０４をＯＳ１上で動作させる。ＯＳ１はＯＳ２のメモリ領域を参照できない為、ユーザ１１は視聴制御プログラム５０３がどのように動作しているかを知ることができない。ユーザ１１が知ることのできるのは、ＵＩ部プログラム５０４が提供する情報のみである。

【００２８】（ＯＳ１とＯＳ２間の通信）図４に示すように、それぞれのＯＳが管理する環境間の通信は、通信制御プログラム５０１がＯＳ２参照領域９の内容を参照することにより実現される。システム起動時に複数ＯＳ制御プログラム８が、ＯＳ２が使用する上記ページテーブルにＯＳ１側にあるＯＳ２参照領域９をマッピングしておくことにより、通信制御プログラム５０１がＯＳ２参照領域９を参照することを可能とする。通信制御プログラム５０１はＵＩ部プログラム５０４がＯＳ２参照領域９に書き込んだ内容をコマンドリスト５０２と比較する。具体的には、ＵＩ部プログラム５０４が情報を受け渡す視聴制御プログラム５０３に関する情報（プログラム名）、制御情報などをＯＳ２参照領域９に書き込む。比較した結果、コマンドリスト５０２にあるコマンドであれば、ＵＩ部プログラム５０４と対となっている視聴制御プログラム５０３にそのコマンドを受け渡す。なお、ＵＩ部プログラム５０４と視聴制御プログラム５０３は１対１対応である必要はない。

【００２９】コマンドリスト５０２には、ＯＳ２上で動作中の視聴制御プログラム５０３が起動時に書き込んだＯＳ１側からの操作を許可しているコマンドがあり、動作していないソフトウェアのコマンドはない。コマンドリスト５０２にないコマンドであれば、後述するＯＳ２からＯＳ１への通信方法を用いて、エラーメッセージをＵＩ部プログラム５０４に渡す。ＵＩ部プログラム５０４は、ＯＳ１が提供する機能を用いて表示または音を用いて、ユーザへのエラー通知を行う。

【００３０】コマンドリスト５０２の内容は、ＯＳ２上で動作している視聴制御プログラム５０３によって変化する。コマンドリスト５０２の書換えは、新たに視聴制御プログラム５０３が起動したときに、その起動した視聴制御プログラム５０３が行う。視聴制御プログラム５０３は、終了するときに、その視聴制御プログラム５０３に対応したコマンドを、コマンドリスト５０２から削除する。

【００３１】ＯＳ２側からＯＳ１側への通信は、通信制御プログラム５０１が視聴制御プログラム５０３から伝達情報を受け取り、その情報をＯＳ２参照領域９に書き込むことにより行う。ＯＳ１上のＵＩ部プログラム５０４は、ＯＳ２参照領域９の内容を参照することによりＯＳ２側からの情報を受け取る。

【００３２】その他の実施例として、視聴制御プログラム５０３毎にあらかじめコマンドリスト５０２を設け、通信制御プログラム５０１は、視聴制御プログラム５０３毎のコマンドリスト５０２と比較することにより通信の制御を行うようにしてもよい。コマンドリスト５０２は、ハードディスクなどの記憶装置に暗号化された状態で保存されていることが望ましい。特開平１１－０８５５４６号公報に開示されている異種ＯＳ上のプロセス間通信を実現する方法を用いても良い。

【００３３】（ハードウェアモジュールの機能及び役割）ハードウェアモジュール３は物理的及び論理的に内部解析や改ざんが防衛された鍵管理機能などをもつ耐タンパハードウェアモジュールである。ハードウェアモジュール３の構成を図５に示す。ハードウェアモジュール３は、ハードウェアモジュール３毎に固有の公開鍵暗号方式における秘密鍵３０１（ｐｒｉｖａｔｅ　ｋｅｙ）と、それに対応する公開鍵３０２と、認定機関の公開鍵３１０と、複数ＯＳ制御プログラム８起動のためのブートプログラム４と、暗号化システムファイル復号鍵３０３と、認証プログラム５と、鍵管理プログラム１９と、コンテンツ鍵１７と、ソフトウェア鍵１８と、付加情報ファイル３０５とを耐タンパ性を備えたメモリの不揮発領域３０９に記憶しておく。

【００３４】コンテンツ鍵１７は暗号化コンテンツの復号鍵であり、ソフトウェア鍵１８は暗号化視聴用ソフトウェアの復号鍵である。付加情報ファイル３０５とは、コンテンツ鍵１７とソフトウェア鍵１８とに関連する、有効期限や使用条件などの情報が書き込まれたファイルである。ハードウェアモジュール３はＣＰＵ３０７、メモリ３０６、外部との通信インタフェース３０８を持ち、外部からの入力に対する処理を行う。コンテンツそのものを不揮発領域３０９に記憶しておいても良い。

【００３５】ハードウェアモジュール３の外部からハードウェアモジュール３内の情報へのアクセスに際しては、起動時を除き、ハードウェアモジュール３が認証プログラム５をＰＣのメモリ１２上に送信し、アクセスしてきたソフトウェアの認証を行う。認証には公開鍵３０２または認定機関の公開鍵３１０を用いる。認証の結果、正しければハードウェアモジュール３は必要な情報をアクセスしてきたソフトウェアに送信し、正しくなければエラーメッセージをアクセスしてきたソフトウェアに送信する。

【００３６】ＰＣの起動時におけるハードウェアモジュール３へのアクセスは、ハードウェアモジュール３は認証プログラム５をＰＣのメモリ１２上に送信し、認証プログラム５はＰＣのメモリ１２上に不要なプロセスが動作していないことを確認し、不要なプロセスが動作していなければ、ハードウェアモジュール３からブートプログラム４を取り出し、ブートプログラム４を実行する。不要なプロセスが動作している場合には、起動を停止する。

【００３７】また、ハードウェアモジュール３へアクセスするソフトウェアが取り出せる情報を制限する。ハードウェアモジュール３内の情報と、その情報を取り出すことが可能なソフトウェアＩＤのテーブルをハードウェアモジュール３内に設ける。鍵管理プログラム１９は、上記テーブルを利用して、ソフトウェア毎に取り出せる情報を制限する。

【００３８】鍵管理プログラム１９は、サーバ２０１からコンテンツ鍵１７またはソフトウェア鍵１８を取得するときに用いる、ランダムに生成した一時的なセッション鍵の生成、暗号化データの復号の処理や、ディジタル署名を用いた認証、後述する鍵の管理を行う。

【００３９】ハードウェアモジュール３毎に固有の秘密鍵３０１は、暗号化ソフトウェアまたは暗号化コンテンツを復号するためコンテンツ鍵１７またはソフトウェア鍵１８の受け渡しなどに利用する。ハードウェアモジュール３毎の固有の秘密鍵３０１、公開鍵３０２を利用することによって、ハードウェアモジュール３毎に異なる暗号をかけてコンテンツ鍵１７またはソフトウェア鍵１８を配布することが可能であり、また、ソフトウェア、コンテンツの不正使用を防止することが可能であり、また、ユーザ毎に異なるサービスを提供することも可能である。

【００４０】ただし、鍵管理プログラム１９に、秘密鍵３０１をハードウェアモジュール３の外部に出力するための命令を用意しないことにより、秘密鍵３０１がハードウェアモジュール３の外部に出力されることを防ぐ。

【００４１】ハードウェアモジュール３は１つのハードウェアモジュール３に上述した全ての機能を含めるのではなく、機能毎に複数のハードウェアモジュール３を用いても良い。例えば、ハードウェアモジュール３を、システムを起動するための情報（ブートプログラム４、認証プログラム５、鍵管理プログラム１９、暗号化システムファイル復号鍵３０３）を持つハードウェアモジュール３Ａと暗号化ソフトウェア及び暗号化コンテンツの鍵管理のための情報（認証プログラム５、秘密鍵３０１、公開鍵３０２、コンテンツ鍵１７、ソフトウェア鍵１８、鍵管理プログラム１９、付加情報ファイル３０５）を持つハードウェアモジュール３Ｂの２つに分けることも可能である。

【００４２】コンテンツ鍵１７、ソフトウェア鍵１８の管理を行っているハードウェアモジュール３ＢをＩＣカードのようなリムーバブル形式にすることにより、１台のＰＣを複数のユーザで共有して、ユーザ毎に異なるコンテンツを視聴することが可能であるし、また、本実施例のシステムが導入されている別のＰＣにおいてもコンテンツを視聴することが可能である。

【００４３】（鍵管理）コンテンツ鍵１７とソフトウェア鍵１８と暗号化システムファイル復号鍵３０３の管理は鍵管理プログラム１９が行う。鍵管理プログラム１９はコンテンツ鍵１７またはソフトウェア鍵１８を、使用条件などの書かれた付加情報ファイル３０５に従い管理する。例えば、使用期限のついた鍵の期限が過ぎた場合には、鍵管理プログラム１９は鍵管理機能により鍵を削除し、その鍵を利用したコンテンツの視聴やソフトウェアの使用を停止することが可能である。

【００４４】この機能を利用することにより、お試し期間を設定し、一定期間だけコンテンツを視聴できるようにしたり、一定期間だけソフトウェアの機能を全て利用できるようにしたりするといったサービスが可能である。コンテンツ鍵１７とソフトウェア鍵１８及び付加情報ファイル３０５をハードウェアモジュール３にて管理することにより、ユーザ１１が不正に書き換えることを防止可能である。

【００４５】（システムのインストール）本実施例のシステムのインストールは、ユーザ１１が持つ既存の一般的なＰＣが備える外部インタフェース（ＵＳＢ、ＰＣカード、拡張ボードなど）にハードウェアモジュール３を接続し、他の媒体（ＣＤＲＯＭなど）に格納されているシステムインストールソフトウェア１４を用いて行う。

【００４６】図２はシステムインストールソフトウェア１４の構成例である。システムインストールソフトウェア１４は平文システムインストールプログラム２２１、暗号化システムファイル２２２、ディジタル署名２２３をもつ。平文システムインストールプログラム２２１は実行中の不要なプロセスを終了させる機能、ハードディスク２０４のパーティション分割機能及び本実施例システムをインストールする機能を持つ。暗号化システムファイル２２２は全体または部分的に暗号化されており、複数ＯＳ制御プログラム８、ＯＳ２が含まれており、必要であればＯＳ１を含んでいても良い。ディジタル署名２２３は、システムインストールソフトウェア１４が改ざんされていないことを確認するために用いるもので、公開鍵３０２で検証可能に生成されている。したがって、ユーザはインストールに際して、ディジタル署名２２３を検証できる公開鍵３０２が格納されたハードウェアモジュール３を入手する必要がある。

【００４７】図１３はシステムインストールの処理の流れである。ステップ１３０１にて、ユーザ１１がＰＣから平文システムインストールプログラム２２１を実行することによりインストールが開始される。ステップ１３

０２にて、平文システムインストールプログラム２２１は実行中のプロセスの確認を行い、不要なプロセスを終了させ、インストール中に重要な情報が盗まれないようにする。ステップ１３０３にて、平文システムインストールプログラム２２１は、暗号化システムファイル復号鍵３０３を取得するための命令を、ハードウェアモジュール３へ送信する。

【００４８】ステップ１３０４にて、ハードウェアモジュール３は受信した命令を実行する前に、認証プログラム５をＰＣのメモリに送信する。認証プログラム５は平文システムインストールプログラム２２１及び暗号化システムファイル２２２のハッシュ値を計算し、計算結果とディジタル署名２２３をハードウェアモジュール３に送信する。鍵管理プログラム１９は送信された計算結果及びディジタル署名２２３と公開鍵３０２を用いて署名検証を行い、正しければ暗号化システムファイル復号鍵３０３を平文システムインストールプログラム２２１に渡し、次のステップに進む。正しくなければ、エラーメッセージを平文システムインストールプログラム２２１に渡し、インストールを中止する。

【００４９】ステップ１３０５にて、平文システムインストールプログラム２２１は暗号化システムファイル復号鍵３０３を用いて、暗号化システムファイル２２２の復号を行う。ステップ１３０６にて、平文システムインストールプログラム２２１は復号後の暗号化システムファイル２２２の中にある設定ファイルを参照しながらシステムのインストールを行う。なお、暗号化システムファイル２２２の中にシステムインストールプログラムを入れておき、暗号化システムファイル２２１の復号後は、暗号化システムファイル２２２の中のシステムインストールプログラムがシステムのインストールを行っても良い。

【００５０】平文システムインストールプログラム２２１はＯＳ１用およびＯＳ２用に領域を確保するためにハードディスク２０４のパーティション分割を行い、ＯＳ１用に確保された領域２０４ａには本実施例のシステム導入前にインストールされていたＯＳ１を含めハードディスク上の情報を全て移し、ＯＳ２用に確保された領域２０４ｂには新たにＯＳ２のインストールを行う。複数ＯＳ制御プログラム８はＯＳ１およびＯＳ２のどちらの領域に書き込んでも良いし、新たに領域を確保して書き込んでも良い。また、ハードディスクドライブを複数台備えたＰＣの場合は、パーティション分割せずに、領域２０４ａ、２０４ｂをそれぞれ別ドライブに割り当てても良い。

【００５１】ユーザ１１による解析および改ざんを防止するために複数ＯＳ制御プログラム８、ＯＳ２の全体または一部を暗号化してハードディスク上に書き込むことが望ましい。同様にＯＳ１も暗号化してハードディスクに書き込んでも良い。また、システムを正常に起動させるために平文システムインストールプログラム２２１はブートプログラム４をハードウェアモジュール３内に書き込む。ハードディスクのマスターブートレコードに、ハードウェアモジュール３から起動するためのプログラムなど必要な情報を書き込んでおく。

【００５２】なお、本実施例のシステムのインストールはＰＣに予めＯＳ１がインストールされていることを前提としているが、ＯＳ１が予めインストールされていなくても、本実施例のシステムを導入することが可能である。さらに、上記システムのインストール方法は本実施例のシステムに限らず、１台のＰＣ上に１つのＯＳをインストールする方法としても利用可能である。

【００５３】（システムの起動）本実施例のシステムが起動するまでの処理を図３に示す。ステップ２３１、２３２にて、ユーザ１１がＰＣの電源を入れることにより、ＰＣのＣＰＵはハードディスクのマスターブートレコードにあるプログラム（初期プログラム）を呼び出す。このプログラムはハードウェアモジュール３内の認証プログラム５をＰＣのメモリ上にロードする。認証プログラム５は他の不要なプロセスが動作していないことを確認する。他の不要なプロセスが動作している場合には起動を停止し、動作していない場合には認証プログラム５はハードウェアモジュール３からブートプログラム４をＰＣのメモリ上に読み込み、ブートプログラム４を実行する。

【００５４】不要なプロセスが動作していないことを確認することにより、不正なユーザが、例えば起動監視プログラムのようなものを実行させたあとで認証プログラムを呼び出すようにマスターブートレコードを書き直し，重要な情報（暗号化システムファイル復号鍵）を盗むことを防止する。ステップ２３３、２３４にて、ブートプログラム４はＰＣのハードディスクから暗号化システムファイルをＰＣのメモリ上にロードし、さらにハードウェアモジュール３から暗号化システムファイル復号鍵３０３を取り出し、暗号化システムファイルの復号を行う。

【００５５】ステップ２３５にて、まず、複数ＯＳ制御プログラム８が各ＯＳのメモリ領域を割り当て、それぞれの領域にＯＳ１及びＯＳ２のシステムファイルを配置する。複数ＯＳ制御プログラム８はＯＳの切り替えの制御を行い、各ＯＳは制御が自分に移ったときにそれぞれに必要な初期設定及びプログラム、データなどをメモリにロードすることにより、起動が終了する。起動が終了すると、ＰＣはユーザ１１がＯＳ１上で操作できる状態となる。

【００５６】（視聴用ソフトウェアのインストール前の構造）本実施例のシステムで利用する視聴用ソフトウェア１０は、予めその一部を、異なる視聴用ソフトウェア個々に固有の鍵を用いて、部分的に暗号化しておく。視聴用ソフトウェア１０のインストール前の構成例を図６

に示す。視聴用ソフトウェア１０はＯＳ１用インストーラ３１１、ＯＳ２用インストーラ３１２、暗号化ソフトウェア３１３、ディジタル署名１６を持つ。ＯＳ１用インストーラ３１１はＯＳ２へ視聴用ソフトウェア１０のインストール要求を出す機能を持ち、ＯＳ１上で動作するプログラムである。ＯＳ２用インストーラ３１２はＯＳ２上で動作するプログラムであり、ハードウェアモジュール３からソフトウェア鍵１８を取り出す機能を持つ。暗号化ソフトウェア３１３はＯＳ２上に視聴用ソフトウェア１０をインストールするためのソフトウェアである。

【００５７】なお、ＯＳ１用インストーラ３１１、ＯＳ２用インストーラ３１２、暗号化ソフトウェア３１３はそれぞれプログラム、データファイル、設定ファイルなどの複数のファイルを持つ。また、暗号化ソフトウェア３１３は全てが暗号化されている必要はなく、解析されたくない部分だけを暗号化していても良いし、使用制限、機能制限を行うために部分的に暗号化していても良い。さらに、暗号化は全てに共通の鍵を用いる必要はなく、視聴用ソフトウェア１０を構成するファイル毎もしくは機能毎に別々の鍵を用いてもよい。ディジタル署名１６は、視聴用ソフトウェア１０の改ざん検知に利用する。また、視聴用ソフトウェア１０の改ざんのみを許さないという場合には、特に視聴用ソフトウェア１０を暗号化する必要はなくディジタル署名１６を用いて改ざん検知を行う。

【００５８】本実施例のシステムに対応した視聴用ソフトウェア１０の配布形態は、既存のソフトウェアと同様に、インターネットなどのネットワーク経由での配布、リムーバブルメディアによる配布など、どのような形態であっても良い。また、本実施例では視聴用ソフトウェアを例としているが、それ以外の解析、改ざんを防止したいソフトウェアであっても良い。

【００５９】（ソフトウェア鍵の取得）ソフトウェア鍵１８の取得方法を図７に示す。ソフトウェア鍵１８の取得は、視聴用ソフトウェア１０のインストール時もしくは視聴用ソフトウェア１０の暗号化されている部分を復号する必要が初めて生じた場合に行う。ステップ３２１において、視聴用ソフトウェア１０はサーバ２０１にハードウェアモジュール３毎に固有の公開鍵３０２（ＫＰと記す）及び公開鍵証明書（公開鍵３０２と併せて保存されていても良い）と、視聴用ソフトウェアが備えているＩＤ情報を送る。サーバ２０１側では公開鍵証明書により、正規のハードウェアモジュールであるかどうかの認証を行う。

【００６０】ステップ３２２において、サーバ２０１側は一時的なセッション鍵Ｋｓ１（共通鍵）を生成し、受信した公開鍵３０２（ＫＰ）を用いて暗号化した結果を、ユーザ１１のＰＣに送信する。ユーザ側のＰＣでは、視聴用ソフトウェア１０が受信データを受け取り、ハードウェアモジュール３に受信データを送信する。

【００６１】ステップ３２３において、ハードウェアモジュール３内の鍵管理プログラム１９は秘密鍵３０１を用いて、そのデータの復号を行いＫｓ１を得るとともに、一時的なセッション鍵Ｋｓ２（共通鍵）を生成し、セッション鍵Ｋｓ１を用いて暗号化してサーバ２０１に送信する。ステップ３２４において、サーバ２０１は、受信データをＫｓ１を用いて復号しＫｓ２を得るとともに、ソフトウェア鍵１８（Ｋｓｏｆｔと記す）とその他の付加情報（使用条件など）を、セッション鍵Ｋｓ２を用いて暗号化して、ユーザ１１のＰＣ１２に送信する。

【００６２】ソフトウェア鍵１８（Ｋｓｏｆｔ）のみを送るのであれば、公開鍵３０２（ＫＰ）を用いてソフトウェア鍵１８（Ｋｓｏｆｔ）を暗号化してユーザ１１のＰＣに送信しても良い。ユーザ１１のＰＣでは、視聴用ソフトウェア１０は、受信したデータをハードウェアモジュール３内またはＰＣのハードディスク上に書き込む。ハードウェアモジュール３内に書き込む場合は、特に暗号化する必要はないので、ハードウェアモジュール３内でセッション鍵Ｋｓ２を用いて復号して書き込んでもよい。一方、ＰＣのハードディスク上に書き込む場合には暗号化した状態で書き込み、ハードウェアモジュール３内にはセッション鍵Ｋｓ２を書き込む。このとき一旦、セッション鍵Ｋｓ２を用いて暗号化されたソフトウェア鍵１８（Ｋｓｏｆｔ）、付加情報を復号し新たに鍵を生成して暗号化しなおしても良い。

（視聴用ソフトウェアのインストール）視聴用ソフトウェア１０のインストールの処理の流れを図６、図８を用いて説明する。ステップ３３１にて、ユーザ１１がＯＳ１用インストーラ３１１を起動する。ステップ３３２にて、ＯＳ１用インストーラ３１１はＯＳ１側にあるＯＳ２参照領域９に視聴用ソフトウェア１０のインストールを行う命令を書き込む。この命令にはＯＳ１側にある視聴用ソフトウェア１０の全部またはＯＳ２上でインストールに必要なファイルの移動またはコピーの命令およびＯＳ２用インストーラ３１２を起動する命令を含む。ステップ３３３にて、通信制御プログラム５０１がＯＳ２参照領域９を参照して書き込まれている命令を実行する。

【００６３】以下の作業はＯＳ２上で行われ、視聴用ソフトウェア１０はＯＳ２上にインストールされる。ステップ３３４にて、ＯＳ２用インストーラ３１２は、まずハードウェアモジュール３に対して、インストールしようとする視聴用ソフトウェアに対応したソフトウェア鍵１８を持っているかどうかを問い合わせる。このときハードウェアモジュール３は認証プログラム５をＰＣ１２のメモリに送信し、認証プログラム５が、視聴用ソフトウェアのハッシュ値を計算してディジタル署名１６と共にハードウェアモジュール３に送る。鍵管理プログラム１９は、送られてきたハッシュ値と認定機関の公開鍵３

１０とディジタル署名１６を用いて視聴用ソフトウェア１０の認証を行い、正当な場合にのみ問合せを受け付ける。正しくない場合にはエラーメッセージをＯＳ２用インストーラに送信する。ＯＳ２側に認証プログラムを用意しておき、ハードウェアモジュール３へのアクセスが発生したときに、その認証プログラムが視聴用ソフトウェア１０の認証を行ってもよい。

【００６４】ハードウェアモジュール３がソフトウェア鍵１８を持っていない場合には、ＯＳ２用インストーラ３１２がサーバ２０１からソフトウェア鍵１８を取得して、ハードウェアモジュール３に渡す。その後に、ＯＳ２用インストーラ３１２は、ハードウェアモジュール３に復号するための命令を送信する。ハードウェアモジュール３がソフトウェア鍵１８を持っている場合にはサーバ２０１への問い合わせをせずに、ハードウェアモジュール３に復号するための命令を送信する。

【００６５】ステップ３３５にて、ハードウェアモジュール３は対応するソフトウェア鍵１８をＯＳ２用インストーラ３１２に送信し、ＯＳ２用インストーラ３１２は復号を行う。本体部は必要な部分だけ復号し、インストール時に復号する必要のない部分は暗号化したままの状態にしておく。また、いったん復号して新たに鍵を生成して再度暗号をかけなおしてもよい。視聴用ソフトウェア１０が暗号化されていない場合や、インストール時に復号する必要のない場合には、ディジタル署名１６を用いた認証を行い、インストールを行う。初めて復号を行う必要が出たときに、ハードウェアモジュール３に対して、ソフトウェア鍵１８を持っているかどうかを問い合わせ、持っていない場合にはサーバ２０１に問い合わせることによって、対応する鍵を取得する。

【００６６】インストーラは、図９に示すようにＯＳ１側のハードディスク２０４ａにＵＩ部プログラム５０４を、ＯＳ２側のハードディスク２０４ｂに本体起動プログラム３４２、暗号化ソフトウェア３４３、ディジタル署名３４４を保存する。本体起動プログラム３４２は暗号化ソフトウェア３４３を復号し、実行する機能をもつ。暗号化ソフトウェア３４３は視聴制御プログラム５０３を含む、視聴用ソフトウェア１０の各種ファイルが暗号化されたものである。暗号化ソフトウェア３４３とディジタル署名３４４はＯＳ１側に書き込んでおいても良い。これらのファイルは全て別々のファイルでなければならないということはなく、１つのファイルの中で分割しておいても良い。

【００６７】視聴用ソフトウェア１０が暗号化されていない場合は、ＯＳ１側にＵＩ部プログラム５０４、ＯＳ２側に平文ソフトウェア本体とディジタル署名３４４を書き込むだけで良い。ディジタル署名３４４は、あらかじめインストールソフトウェアの中に組み込んでおいても良いし、インストール時に新たに作成しても良いし、これらを併用しても良い。インストール時に作成する場合、インストール後のソフトウェアのハッシュ値を計算し、これをハードウェアモジュール３に送信して、ハードウェアモジュール３内の秘密鍵３０１によって暗号化し、ディジタル署名３４４を作成する。

【００６８】また、ＯＳ１側に書き込まれるファイルとＯＳ２側に書き込まれるファイル、すなわちＵＩ部プログラム５０４と本体起動プログラム３４２、暗号化ソフトウェア３４３は、必ずしも１対１に対応している必要はない。ＵＩ部プログラム５０４は、ユーザ１１へのインタフェースを提供しているもので変更、交換しても、セキュリティには影響しない。ＯＳ２側上で動作するソフトウェアのインタフェースを公開することにより、ユーザ１１はＵＩ部プログラム５０４を自由に作成することが可能である。

【００６９】（視聴用ソフトウェアのライセンス契約）視聴用ソフトウェア１０のライセンス契約の方法は、視聴用ソフトウェア１０が暗号化されている場合とされていない場合とに分けることができる。視聴用ソフトウェア１０が暗号化されている場合、復号鍵を取得するときにライセンス契約を行うことが可能である。視聴用ソフトウェア１０が暗号化されていない場合でライセンス契約が必要な場合には、視聴用ソフトウェア１０のライセンス契約をしたか、していないかを判断する部分にディジタル署名をつける。

【００７０】鍵管理プログラム１９は、このディジタル署名を秘密鍵３０１を用いてハードウェアモジュール３内で作成し、ハードディスク上またはハードウェアモジュール３内に書き込む。ライセンス契約が結ばれた場合には、ライセンス契約をしたか、していないかを判断する部分を書換えるとともに、ディジタル署名も付けなおす。ディジタル署名を用いることにより、ユーザ１１による改ざんを防止でき、ユーザ１１が不正に視聴用ソフトウェア１０を利用することを防止できる。

【００７１】（視聴用ソフトウェアの起動）視聴用ソフトウェア１０の起動の流れを図１０に示す。ステップ４０１にて、ユーザ１１がＵＩ部プログラム５０４を実行することにより、ＵＩ部プログラム５０４はＯＳ２参照領域９に本体起動プログラム３４２を起動する命令を書き込む。ＵＩ部プログラム５０４の起動は、ファイル管理ソフトウェアを用いたり、画面上のアイコンを操作することなどにより行う。ステップ４０２にて、通信制御プログラム５０１がＯＳ２参照領域９を参照し、本体起動プログラム３４２を実行する。ステップ４０３にて、本体起動プログラム３４２は暗号化ソフトウェア３４３を復号するために、ハードウェアモジュール３からソフトウェア鍵１８を取り出し、暗号化ソフトウェア３４３を復号する。復号された暗号化ソフトウェア３４３は視聴制御プログラム５０３及び各種設定ファイルなどに分かれる。

【００７２】このとき、ハードウェアモジュール３は、

まず、本体起動プログラム３４２の認証を、ディジタル署名３４４を用いて、上述のステップ１３０４と同様に行い、認証できれば命令を受け付けて、ソフトウェア鍵１８を本体起動プログラム３４２に送信する。具体的には、ハードウェアモジュール３は受信した命令を実行する前に、認証プログラム５をＰＣのメモリに送信する。認証プログラム５は本体起動プログラム３４２及び暗号化ソフトウェア３４３のハッシュ値を計算し、計算結果とディジタル署名３４４をハードウェアモジュール３に送信する。鍵管理プログラム１９は送信された計算結果及びディジタル署名３４４と公開鍵３０２を用いて署名検証を行い、正しければソフトウェア鍵１８を本体起動プログラム３４２に渡し、次のステップに進む。正しくなければ、エラーメッセージを本体起動プログラム３４２に渡し、起動を中止する。

【００７３】本体起動プログラム３４２の認証は、ＯＳ２側にあるハードウェアモジュール３のデバイスドライバ、もしくは認証プログラムを用いて行ってもよい。また、暗号化ソフトウェア３４３の一部が暗号化されている場合においても起動時に暗号化部を復号する必要がない場合や使用条件によりある特定の機能を使用できない場合には、暗号化部はそのままにしておき、視聴用ソフトウェア１０を起動しても良い。この場合は必要なときに使用条件に反していなければ暗号化部を復号する。

【００７４】ステップ４０４にて、視聴制御プログラム５０３が設定ファイルを読み込み、視聴用ソフトウェア１０の起動が終了したメッセージをＵＩ部プログラム５０４に送信する。ＵＩ部プログラム５０４がメッセージを受け取った段階で、ユーザ１１による視聴のための操作を待つ状態となる。

【００７５】（視聴用ソフトウェアの制御）視聴用ソフトウェア１０の起動後は、視聴制御プログラム５０３が、ＯＳ１側から視聴制御プログラム５０３を制御するためのコマンドを、コマンドリスト５０２に追加する。ここで追加するコマンドは視聴制御プログラム５０３が一時的に書き込むものであり、終了時はコマンドリストから削除する。ＵＩ部プログラム５０４は、ユーザ１１からの操作（コンテンツの再生、停止、コンテンツタイトルの選択など）を受け取り、ＯＳ２参照領域９に視聴制御プログラム５０３の制御コマンドを書き込む。書き込まれたコマンドを通信制御プログラム５０１が読み取り、コマンドリスト５０２に載っているコマンドであれば、視聴制御プログラム５０３にコマンドを受け渡す。コマンドリスト５０２に載っていないコマンドであれば、通信制御プログラム５０１はエラーメッセージをＯＳ２参照領域９に書き込み、ＵＩ部プログラム５０４に受け渡す。ＵＩ部プログラム５０４は、ＯＳ１が提供する機能を用いて表示または音を用いて、ユーザへのエラー通知を行う。

【００７６】視聴制御プログラム５０３は受け取ったコマンドを処理し、必要であれば結果を画面出力あるいは音出力などを行う。このときのデバイスの制御はＯＳ２が行う。

【００７７】画面出力及び音出力に利用するデバイス（サウンドボード、ビデオボードなど）をＯＳ１及びＯＳ２の両方からアクセスを行うために、複数ＯＳ制御プログラム８がこれらのデバイスの排他制御を行う。具体的には、複数ＯＳ制御プログラム８がデバイスの制御権を管理する。各ＯＳはこれらのデバイスを使用する必要が出た場合に、複数ＯＳ制御プログラム８に割込みを発生させ、複数ＯＳ制御プログラム８はデバイスの制御権を切替える。

【００７８】（コンテンツの配布）コンテンツの配布にはリムーバブルメディアによる配布、通信メディアまたは放送メディアによる配布など様々な形態が考えられる。コンテンツが有料である場合や視聴に制限のある場合など必要に応じてコンテンツを暗号化して配布する。コンテンツを暗号化して配布する場合にはコンテンツ固有の鍵（コンテンツ鍵１７）により暗号化する。ＰＣ１２にコンテンツを保存する場合は、ＯＳ１、ＯＳ２のどちらが管理する領域に保存しても良いし、ハードウェアモジュール３内に保存しても良い。

【００７９】通信メディアまたは放送メディアにより配布されたコンテンツをＯＳ２側またはハードウェアモジュール３内への保存するには、上述の視聴用ソフトウェアと同様の構成を備えたダウンロード用ソフトウェアを設け、ダウンロードと同時にＯＳ２上またはハードウェアモジュール３内に保存することにより可能となる。同様に、ＯＳ１上に保存されているコンテンツをＯＳ２上またはハードウェアモジュール３上に保存するには、上述の視聴用ソフトウェアと同様の構成を備えたファイル管理ソフトウェアを設け、ＯＳ１上のコンテンツをＯＳ２上またはハードウェアモジュール３上に移動、またはコピーを行うことにより、可能となる。

【００８０】さらに、上述のファイル管理ソフトウェアを用いることにより、ＯＳ２上またはハードウェアモジュール３上にあるファイルをＯＳ１側から管理することが可能になる。具体的には、ファイルの内容を変更することはできないが、ユーザが再生したいコンテンツを選択して、視聴用ソフトウェア１０による再生を行わせたり、ファイル名を変更したりすることが可能になる。

【００８１】（コンテンツ鍵の取得）コンテンツ鍵１７の取得方法を図１１に示す。ステップ４１１において、暗号化コンテンツを再生する視聴用ソフトウェア１０はサーバ２０１にハードウェアモジュール３毎に固有の公開鍵３０２（ＫＰ）及び公開鍵証明書（公開鍵３０２と併せて保存されていても良い）と、コンテンツのＩＤ情報を送る。サーバ２０１側では公開鍵証明書により、正規のハードウェアモジュール３であるかどうかの認証を行う。

【００８２】ステップ４１２において、サーバ２０１側は一時的なセッション鍵Ｋｓ１（共通鍵）を生成し、受信した公開鍵３０２（ＫＰ）を用いて暗号化した結果を、ユーザ１１のＰＣに送信する。ユーザ１１側のＰＣでは、視聴用ソフトウェア１０が受信データを受け取り、ハードウェアモジュール３内に受信データを送信する。ステップ４１３において、ハードウェアモジュール３内の鍵管理プログラム１９は秘密鍵３０１を用いて、そのデータの復号を行いＫｓ１を得るとともに、一時的なセッション鍵Ｋｓ２（共通鍵）を生成し、セッション鍵Ｋｓ１を用いて暗号化してサーバ２０１に送信する。ステップ４１４において、サーバ２０１は、受信データをＫｓ１を用いて復号しＫｓ２を得るとともに、コンテンツ鍵１７（Ｋｃと記す）とその他の付加情報（使用条件など）を、セッション鍵Ｋｓ２を用いて暗号化して、ユーザ１１のＰＣ１２に送信する。

【００８３】使用条件には鍵の有効期限などの情報が含まれる。また、コンテンツ鍵１７（Ｋｃ）のみを送るのであれば、公開鍵３０２（ＫＰ）を用いてコンテンツ鍵１７（Ｋｃ）を暗号化してユーザ１１のＰＣに送信しても良い。ユーザ１１のＰＣでは、視聴用ソフトウェア１０は、受信したデータをハードウェアモジュール３内またはＰＣのハードディスク上に書き込む。ハードウェアモジュール３内に書き込む場合は、特に暗号化する必要はないので、ハードウェアモジュール３内でセッション鍵Ｋｓ２を用いて復号して書き込んでもよい。一方、ＰＣのハードディスク上に書き込む場合には暗号化した状態で書き込み、ハードウェアモジュール３内にはセッション鍵Ｋｓ２を書き込む。このとき一旦、セッション鍵Ｋｓ２を用いて暗号化されたコンテンツ鍵１７（Ｋｃ）、付加情報を復号し新たに鍵を生成して暗号化しなおしても良い。

【００８４】（コンテンツの視聴）コンテンツ視聴までの流れを図１２に示す。ステップ４２１において、ユーザ１１の操作によりＵＩ部プログラム５０４は本体起動プログラム３４２の起動命令をＯＳ２参照領域９に書き込む。ステップ４２２において、通信制御プログラム５０１がこの起動命令をＯＳ２参照領域９から読み込み、本体起動プログラム３４２を起動する。本体起動プログラム３４２は暗号化ソフトウェア３４３を復号して、視聴制御プログラム５０３を起動させる。ステップ４２３において、ユーザ１１がＵＩ部プログラム５０４を利用して視聴したいコンテンツタイトルを選択することにより、ＵＩ部プログラムがＯＳ２参照領域９にその情報を書き込む。

【００８５】ステップ４２４にて、通信制御プログラム５０１がその情報を受け取り、視聴制御プログラム５０３にその情報を渡し、視聴制御プログラム５０３がコンテンツをハードディスクからＰＣのメモリ上にロードする。ステップ４２５において、コンテンツが暗号化されている場合、視聴制御プログラム５０３は、対応したコンテンツ鍵１７が存在するかどうかをハードウェアモジュール３に問い合わせ、コンテンツ鍵１７が存在しない場合には再生を中止するか、またはコンテンツ鍵１７を取得するかどうかをユーザ１１に選択させる。

【００８６】コンテンツ鍵１７を取得する場合には、サーバ２０１に問い合わせコンテンツ鍵１７を取得する。取得後に視聴制御プログラム５０３はコンテンツ鍵１７を取り出すための要求をハードウェアモジュール３に送信する。ハードウェアモジュール３内の鍵管理プログラム１９は、付加情報ファイル３０５に書かれている利用条件のチェックを行い、利用条件を満足する場合に限りコンテンツ鍵１７を視聴制御プログラム５０３に渡す。視聴制御プログラム５０３は受け取ったコンテンツ鍵１７を用いてコンテンツの復号を行う。また、コンテンツが暗号化されていない場合には、ステップ４２７へ進む。ステップ４２７にて、視聴制御プログラム５０３は、コンテンツを再生する。コンテンツが映像の場合であればディスプレイ１３に出力する。コンテンツが音を伴う場合であればスピーカにも出力する。

【００８７】上述の実施例によれば、改ざんや不正解析を防ぐことが可能になる。加えて、ＰＣのＣＰＵなどの半導体装置や物理デバイスが、耐タンパ性を持つ内部領域に秘密鍵と公開鍵を格納しておき、データの送受信に際して、公開鍵の交換とセッション鍵の受け渡しとセッション鍵によるデータの暗号化を行えば、装置内のバス上を流れるデータをを横取りされるという問題を解決することが可能になり、更に高いレベルで改ざんや不正解析を防ぐことが可能になる。更に、ＣＰＵや各デバイスは自分の持つ秘密鍵を外部に出力せず、プログラム及びデータをハードディスク上に保存する場合にはＣＰＵの公開鍵を用いて暗号化し、読み込むときはＣＰＵの秘密鍵を用いて復号化することが望ましい。

【００８８】本実施例によれば、アプリケーションソフトウェアとその動作環境の改ざん、不正操作、不正解析を困難にすることが可能になる。不正なユーザによるアプリケーションソフトウェアの解析、改ざん行為ができないため、著作権保護を考慮に入れたコンテンツ視聴ソフトウェアの場合であれば、コンテンツの著作権を保護することが可能である。著作者は不正コピーなどによる著作権侵害を心配することなく良質のコンテンツを提供することが可能になる。ユーザにとってはＰＣ上で良質のコンテンツを楽しむことが可能となり、ソフトウェアのバージョンアップも可能であることから常に最新の機能およびサービスを利用することが可能になる。メーカにとっては専用ハードウェアに比べて経費を削減すると共に、新製品およびサービスをユーザに即提供することが可能になる。ＩＣカードなどのリムーバブルメディアを利用することによって、視聴権のあるコンテンツに対しては、別のＰＣもしくは携帯端末などでもコンテンツ

を視聴することが可能になる。

【００８９】

【発明の効果】耐タンパ性を備えた、ソフトウェアやそれを動作させるシステムを提供できる。

【００９０】

【符号の説明】

３・・・ハードウェアモジュール、４・・・ブートプログラム、５・・・認証プログラム、８・・・複数ＯＳ制御プログラム、９・・・ＯＳ２参照領域、１０・・・視聴用ソフトウェア、１１・・・ユーザ、１３・・・ディスプレイ、１４・・・システムインストールソフトウェア、１６・・・視聴用ソフトウェアのインストール前のディジタル署名、１７・・・コンテンツ鍵、１８・・・ソフトウェア鍵、１９・・・鍵管理プログラム、２０１・・・サーバ、２２３・・・システムインストールソフトウェアのディジタル署名、３０１・・・秘密鍵、３０２・・・公開鍵、３０３・・・暗号化システムファイル復号鍵、３１１・・・ＯＳ１用インストーラ、３１２・・・ＯＳ２用インストーラ、３１３・・・暗号化ソフトウェア、３４２・・・本体起動プログラム、３４４・・・視聴用ソフトウェアのインストール後のディジタル署名、５０１・・・通信制御プログラム、５０２・・・コ＊マンドリスト、５０３・・・視聴制御プログラム、５０４・・・ＵＩ部プログラム。

【図面の簡単な説明】

【図１】耐タンパソフトウェアシステムの全体図。

【図２】システムインストールソフトウェアの構造を示す図。

【図３】システム起動までの処理を示す図。

【図４】ＯＳ１とＯＳ２間の通信方法を示す図である。

【図５】ハードウェアモジュールの構造を示す図である。

【図６】配布ソフトウェアの構造を示す図である。

【図７】ソフトウェア鍵取得までの処理を示す図である。

【図８】ソフトウェアのインストールの処理を示す図である。

【図９】ハードディスク内でのソフトウェアの状態を示す図である。

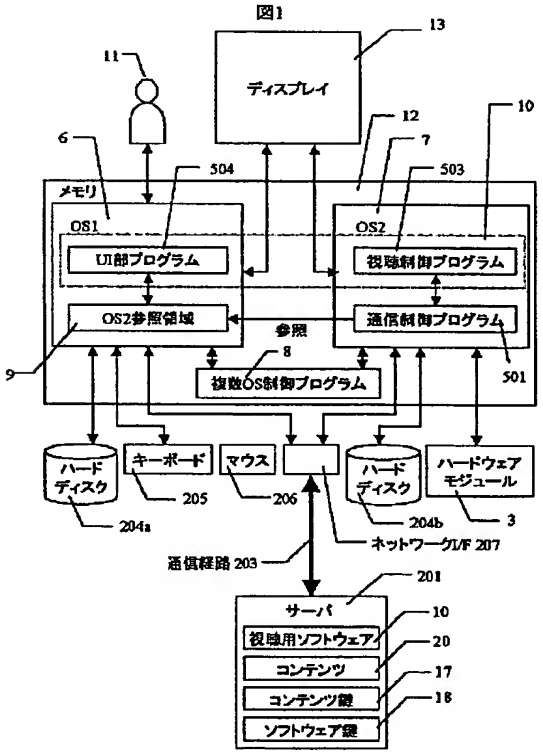
【図１０】ソフトウェア起動の処理を示す図である。

【図１１】コンテンツ鍵取得の処理を示す図である。

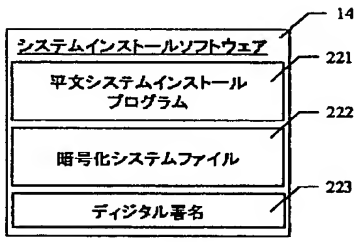
【図１２】コンテンツ視聴の処理を示す図である。

【図１３】システムのインストールの処理を示す図である。

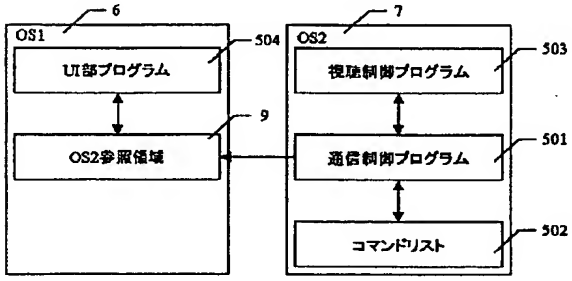
【図１】



【図２】

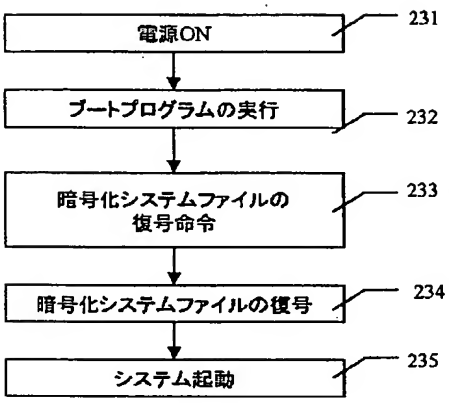


【図４】



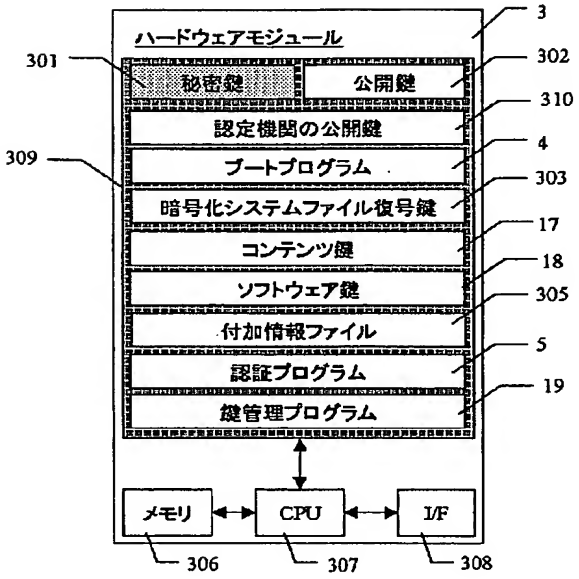
【図３】

図3



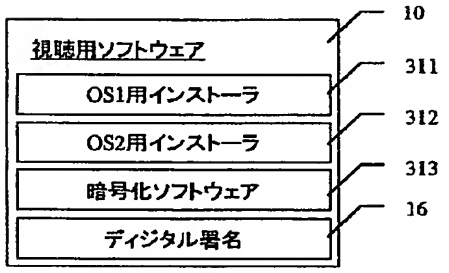
【図５】

図5



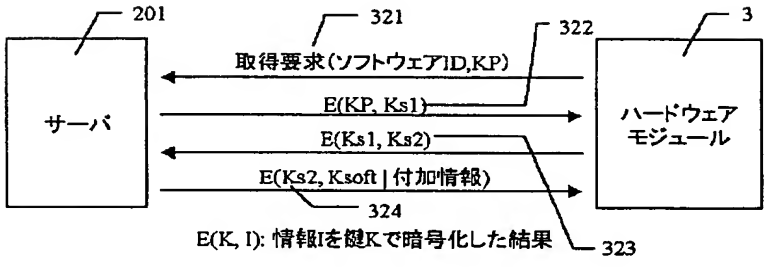
【図６】

図6



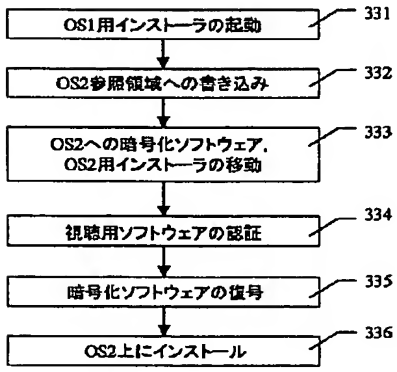
【図７】

図7



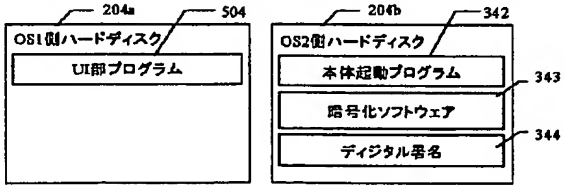
【図８】

図8



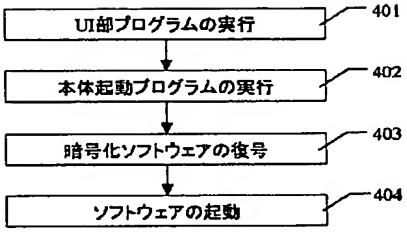
【図９】

図9



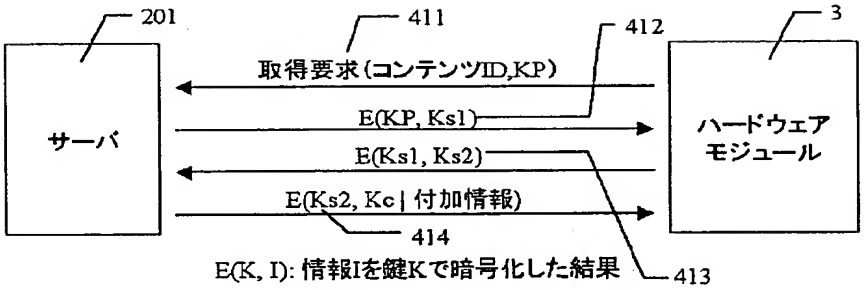
【図１０】

図10



【図１１】

図11



【図１２】

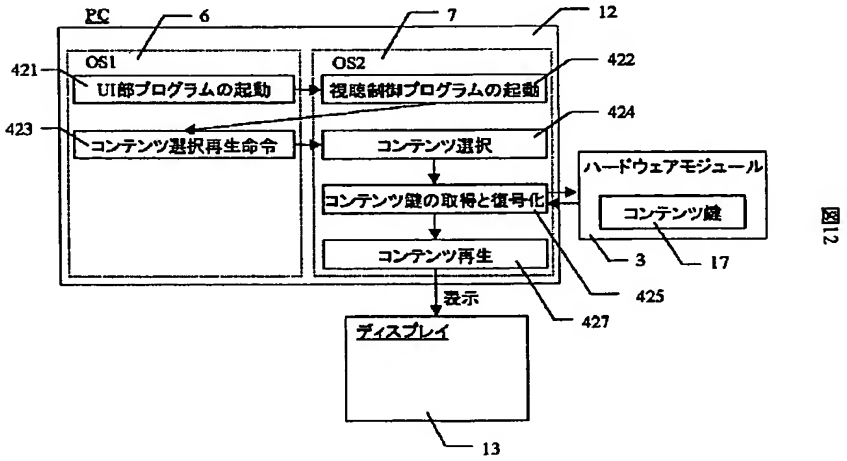
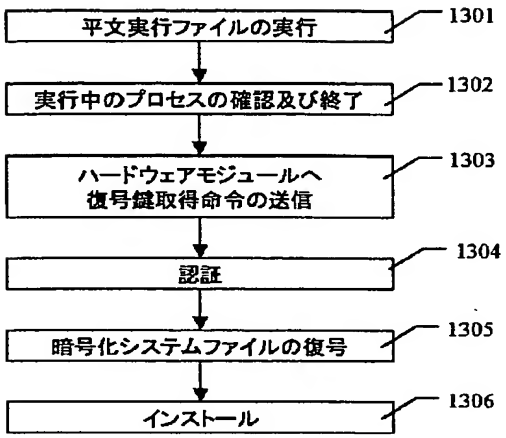


図12

【図１３】

図13



フロントページの続き

(72)発明者　岡本　宏夫
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考)　5B017 AA03 AA06 BA07 BA09 CA09 CA15
5B035 AA13 BB09 BC00 CA11
5B076 AA13 BA10 FA20 FB02